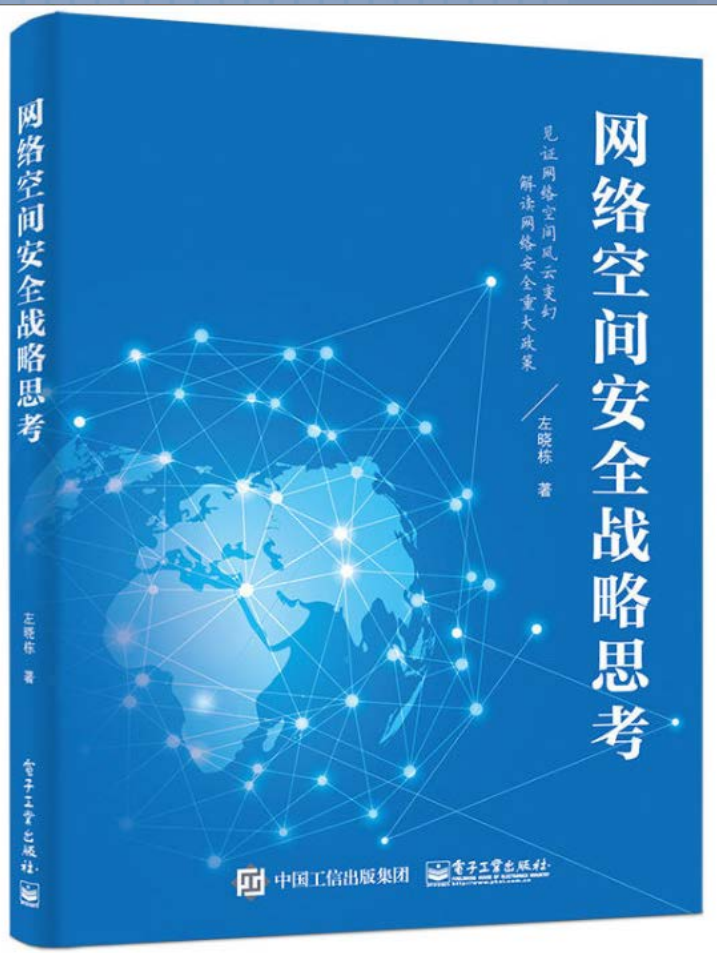
OWASP
Open Web Application Security Project

OWASP ASVS 项目分享

王厚奎
OWASP广西区域负责人
广西网络信息安全服务研究院副院长



信息名称： 关于加强网络安全学科建设和人才培养的意见

信息索引： 360A08-07-2016-0015-1 **生成日期：** 2016-06-12 **发文机构：**

发文字号： 中网办发文〔2016〕4号 **信息类别：** 高等教育

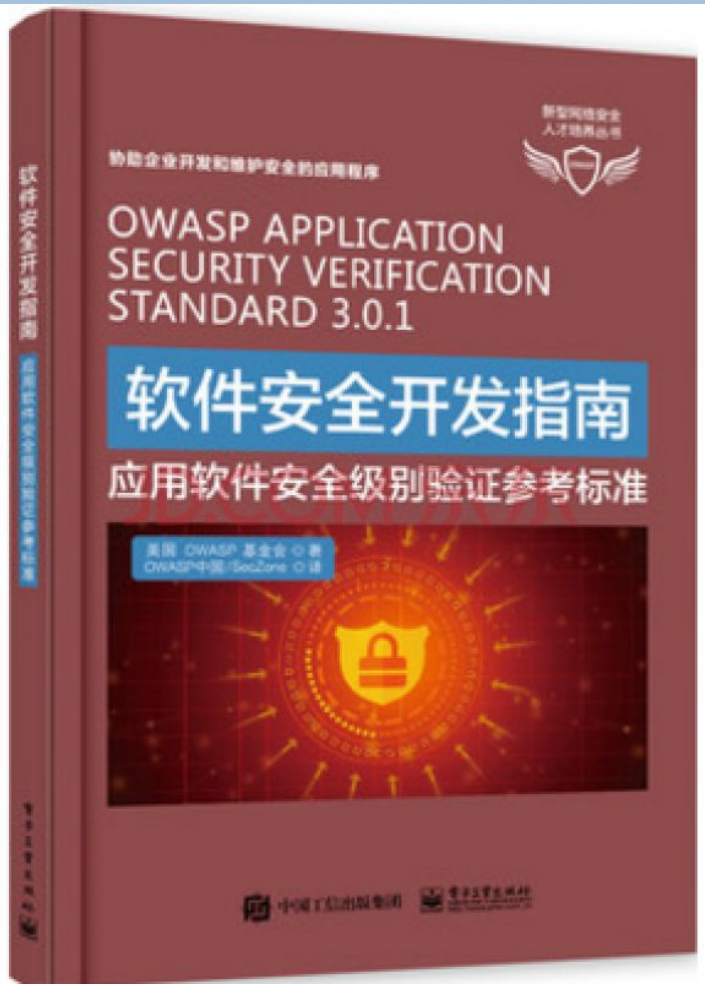
内容概述： 为加强网络安全学院学科专业建设和人才培养，经中央网络安全和信息化领导小

关于加强网络安全学科建设和人才培养的意见

中网办发文〔2016〕4号

OWASP
Open Web Application Security Project

OWASP ASVS



OWASP
Open Web Application
Security Project

软件研发项目主管

软件安全开发服务咨询

网络安全核心专家

高校软件专业和网络安全专业教育工作者

对软件安全感兴趣的个人

- 度量标准：为应用程序开发人员和应用程序所有者提供一个参考标准，以评估应用程序的可信任程度；
- 安全指导：为应用程序中安全控制的开发人员提供有关构建安全控制的指导建议，以满足应用程序的安全开发需求；
- 采购要求：为应用程序的采购合同，提供应用程序安全验证需求的参考标准。

目 录

- 第 1 章　使用应用安全验证标准
- 第 2 章　评估软件达到验证水平

控制目标和验证要求					
V1：架构、设计和威胁建模	V2：认证	V3：会话管理	V4：访问控制	V5：恶意输入处理	V6：密码学安全
V7：错误处理和日志记录	V8：数据保护	V9：通信安全	V10：HTTP安全配置	V11：恶意控件	V12：业务逻辑
V13：文件和资源	V14：移动应用程序	V15：WEB服务	V16：安全配置		

- 第 19 章ASVS的实践案例

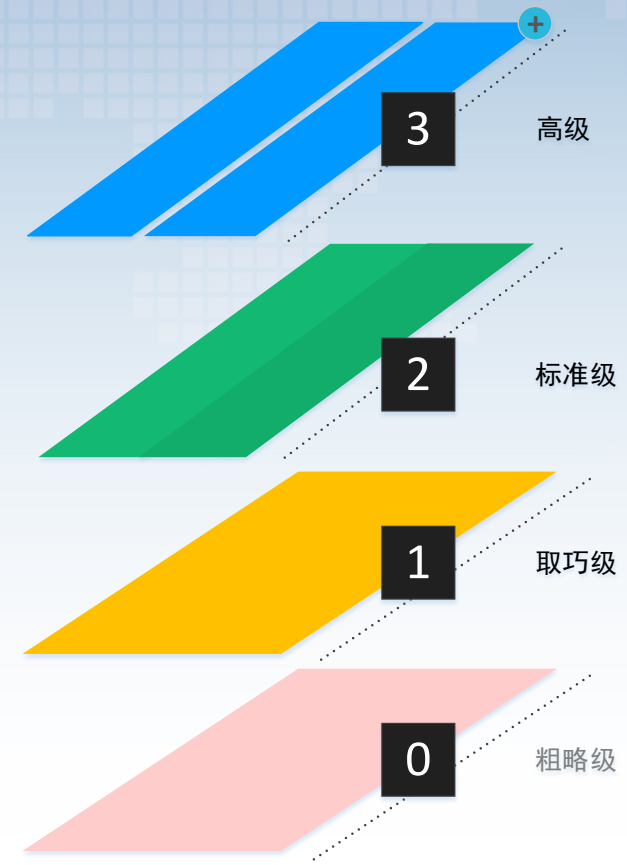
第1章 使用应用安全验证标准

本标准有两个主要目标：

- 帮助组织开发和维护安全的应用程序；
- 允许安全服务提供商、安全工具厂商和终端用户调整应用程序的安全要求和功能。

第1章 使用应用安全验证标准

ASVS为1级及以上验证标准定义了详细的验证要求；而0级验证标准是灵活的、可定制的。



OWASP
Open Web Application Security Project

第1章 使用应用安全验证标准

如何使用这个标准？

- 如果应用程序充分防范《OWASP Top 10》和其他类似清单中包含的安全漏洞，它就实现了ASVS 1级（或取巧级）。
- 如果应用程序能够充分抵御当前与软件相关的大部分风险，那么应用程序就实现了ASVS 2级（或标准级）。
- 如果应用程序充分防范高级的安全漏洞，并且还展示了良好的安全设计原则，它就达到了ASVS 3级验证标准。

第1章 使用应用安全验证标准

如何使用这个标准？

- ASVS 3级需要比所有其他级别更深入的分析、架构、编码和测试。安全应用程序以有意义的方式进行模块化（以促进例如弹性，可扩展性以及最重要的安全层），并且每个模块（由网络连接或物理实例分隔）负责其自身的安全责任（防御深入），这需要妥善记录。责任包括确保机密性（例如：加密）、完整性（例如：交易、输入验证）、可用性（例如：正常处理负载）、认证（包括系统之间）、不可否认性、授权、审计和日志记录的控制。

第1章 使用应用安全验证标准

行业	威胁概要	1级建议	2级建议	3级建议
金融和保险	尽管这一阶段将经历取巧类型的攻击者的尝试，但它通常被认为是一个高价值的攻击目标，攻击者通常是出于经济动机。攻击者通常会寻找敏感的数据或帐户凭证，这些数据可以被用来进行欺诈，或者通过利用内置在应用程序中的资金转移功能来直接获利。技术方面通常包括被窃取证书、应用级别的攻击和社会工程学。一些主要的合规事项包括支付卡行业数据安全标准（PCI DSS）、金融现代化法案（Gramm Leech Bliley Act）和萨班斯-奥克斯利法案（SOX）。	所有网络可访问的应用程序。	包含敏感信息的应用程序（例如：信用卡号码、个人信息）可以以有限的方式转移有限的金额。示例包括：（i）在同一机构的账户之间转账；（ii）具有交易限额的较慢形式的货币流动（例如：ACH）；（iii）在一段时间内具有强制转移限制的电汇。	包含大量敏感信息、允许快速转移大量资金（例如：电汇）、以个别交易形式转移大量资金作为一批较小转账的应用程序。

第1章 使用应用安全验证标准

行业	威胁概要	1级建议	2级建议	3级建议
制造、交通运输、技术、公用事业、基础设施和国防	这些行业看起来有很大差异，但是可能在一个阶段，社工威胁更有可能以更多的时间、技能和资源进行集中攻击组织。因为敏感信息或系统不容易定位，需要利用到内部人员和社会工程学技术。攻击可能涉及内部人员，外部人员或两者之间的勾结。他们的目标可能包括获得知识产权的战略或技术优势。我们也不想忽视攻击者滥用应用功能来影响敏感信息系统的行为或中断敏感信息系统。大多数攻击者正在寻找可用于直接或间接获利的敏感数据，包括个人身份信息和付款数据。这些数据可用于身份盗用，欺诈付款或各种欺诈计划。	所有网络可访问的应用程序。	应用程序包含内部信息或员工的可利用在社会工程学攻击方面的信息。应用程序包含非必要的、但重要的知识产权或商业秘密。	包含有价值的知识产权、商业秘密或政府机密（例如：在美国，这可能是秘密或以上的任何分类）的应用程序对于组织的生存或成功至关重要。控制敏感功能的应用（例如：运输、制造设备、控制系统）或有可能威胁生命安全的应用程序。

第1章 使用应用安全验证标准

行业	威胁概要	1级建议	2级建议	3级建议
医疗	大多数攻击者正在寻找可用于直接或间接获利的敏感数据，以包括个人身份信息和付款数据。这些数据可用于身份盗用，欺诈付款或各种欺诈计划。 对于美国医疗保健行业，健康保险的便携性和责任法案（HIPAA）隐私、安全、违规通知规则和患者安全规则。	所有网络可访问的应用程序	具有少量或中等数量的敏感医疗信息（受保护的健康信息）、个人身份信息或付款数据的应用程序。	应用程序用来控制医疗设备或可能危及人类生命的设备。支付和销售点系统（POS）含有大量的交易数据，可以用来提交欺诈。欺诈通过任何这些应用程序的管理界面进行。

第1章 使用应用安全验证标准

行业	威胁概要	1级建议	2级建议	3级建议
零售、食品、酒店	这一部分的许多攻击者利用投机取巧的“粉碎和抢夺”战术。然而，对于已知含有付款信息，执行金融交易或存储个人身份信息的应用程序，也存在针对特定攻击的常规威胁。虽然不如上述威胁的可能性更大，但也有可能会采取更为先进的威胁来攻击这个行业，窃取知识产权，获得竞争情报，或者与目标组织或商业伙伴在谈判中获得优势。	所有网络可访问的应用程序	适用于商业应用，产品目录信息，内部公司信息和具有有限用户信息（例如：联系信息）的应用程序。具有少量或中等数量的付款数据或结帐功能的应用程序。	支付和销售系统（POS），其中包含可用于提交欺诈的大量交易数据。这包括这些应用程序的任何管理界面。具有大量敏感信息的应用程序，如完整的信用卡号码、姓名、社保号码等。

第 2 章 评估软件达到验证水平

- 《OWASP应用程序安全性验证标准》可用作应用程序的开放式验证标准，包括无限制地访问关键资源（如：架构师、开发人员）、项目文档、源代码、验证的访问测试系统（包括各角色至少访问一个帐户），特别是ASVS 2级和ASVS 3级验证标准。

第 2 章 评估软件达到验证水平

- 保存详细的工作文件、屏幕截图或电影、可靠的和重复暴露问题的脚本、电子测试记录（例如：代理日志、相关注释等）被认为是标准行业实践，并且可以作为开发者非常有用的研究证据。简单地运行工具并报告失败是不够的，这不能够提供足够的证据来证明所有的认证级别问题已经过彻底的测试。如有争议，应有足够的证据证明每一个经过验证的要求都经过测试。

第 3 章 V1：架构、设计和威胁建模

控制目标

- 经过验证的应用程序，需确保满足如下高级别要求：
- ASVS 1级：需识别应用程序中所有的组件，并明确应用程序中使用该组件的原因；
- ASVS 2级：应用程序已定义架构，并且代码遵循架构设计；
- ASVS 3级：架构及设计方案具体落地、实施并有效地应用于程序中。

第 3 章 V1：架构、设计和威胁建模

序号	验证要求描述	1级	2级	3级	原文序号
1	验证是否所有应用程序组件已被识别，且此组件为应用程序必须的组件。	✓	✓	✓	1.1
2	验证是否应用程序所依赖的组件已被识别，如库、模块和外部系统（这些组件不是此应用程序的一部分，但应用程序的操作依赖于它们）。		✓	✓	1.2
3	验证是否应用程序已定义了高级别架构。		✓	✓	1.3
4	验证是否所有应用程序组件都是根据它们提供的业务功能和安全功能来定义的。			✓	1.4
5	验证所有不是应用程序的组件，但是应用程序所依赖的组件是根据它们提供的功能和安全功能来定义的。			✓	1.5

第 3 章 V1：架构、设计和威胁建模

序号	验证要求描述	1级	2级	3级	原文序号
6	验证目标应用程序的威胁模型是否已生成，并覆盖与欺骗、篡改、拒绝、信息泄露、拒绝服务和特权提升（STRIDE）相关的风险。			✓	1.6
7	验证所有的安全控制（包括调用外部安全服务的库）都采用集中化的方式实现。		✓	✓	1.7
8	验证组件是否通过使用已定义的安全控制彼实现相互隔离（例如：网络分段、防火墙规则、基于云的安全组）。		✓	✓	1.8
9	验证是否应用程序在数据层、控制器层和显示层之间有明确的分离，以便安全决策可以在受信任的系统上执行。		✓	✓	1.9
10	验证是否在客户端代码中存有敏感的业务逻辑、秘密密钥或者其他所有权信息。		✓	✓	1.10
11	验证是否所有应用程序组件、库、模块、框架、平台和操作系统中存有已知漏洞。		✓	✓	1.11

第 4 章 V2：认证

控制目标

- 认证是一种用以建立或者确认某件事物（或者某个人）是否如其所声称的或本身具有的真实行为。确保经验证后的应用程序满足如下高级别要求：
- 验证通信发送者的数字身份标识；
- 确保仅授权的实体能够以安全的方式进行身份认证和凭证传输。

第 4 章 V2：认证

序号	验证要求描述	1级	2级	3级	原文序号
1	验证所有的页面和资源在默认情况下需要认证（除了公共目的的页面或资源）。	✓	✓	✓	2.1
2	验证应用程序没有填写了包含凭证的表单。应用程序的预填充，意味着凭证是以明文或可逆的格式存储，这是明确禁止的。	✓	✓	✓	2.2
3	验证所有认证控制强制在服务器端执行。	✓	✓	✓	2.4
4	验证所有认证控制安全地失败，以确保攻击者无法登录	✓	✓	✓	2.6
5	验证密码输入字段允许或鼓励使用密码短语，并且不阻止密码管理器、长密码短语或者高复杂密码的输入。	✓	✓	✓	2.7
6	验证所有可重新获得帐户访问的帐户身份验证功能（例如：更新配置文件、忘记密码、禁用或丢失令牌、帮助桌面或IVR）是否可作为主要的身份认证机制来抵抗攻击。	✓	✓	✓	2.8

第 4 章 V2：认证

序号	验证要求描述	1级	2级	3级	原文序号
7	验证更改密码功能包含“旧密码”、“新密码”和“密码确认”。	✓	✓	✓	2.9
8	验证是否所有认证判断结果均被记录，而不存储敏感的会话标识符或密码。日志应包含安全调查所需的相关元数据		✓	✓	2.12
9	验证帐户密码是否以加盐的方式　哈希存储，并且确保实施充分的工作以抵挡暴力攻击和密码散列恢复攻击。		✓	✓	2.13
10	验证凭证是否通过适当的加密链接方式传输，并且所有要求用户输入凭证的页面或函数都使用了加密链接的方式完成。	✓	✓	✓	2.16
11	验证忘记密码函数功能和其他恢复路径不应泄露用户当前的密码，并且新密码不应以明文形式发送给用户。	✓	✓	✓	2.17
12	验证信息枚举不能通过登录、密码重置或忘记帐号功能进行。	✓	✓	✓	2.18

第 4 章 V2：认证

序号	验证要求描述	1级	2级	3级	原文序号
13	验证应用程序框架或应用程序使用的任何组件没有使用默认的密码（例如：“admin/password”）。	✓	✓	✓	2.19
14	验证反自动化功能是否落地，以有效防止破坏凭证测试、暴力破解和帐户锁定攻击。	✓	✓	✓	2.20
15	验证用于访问外部服务的应用程序，其所有认证凭证是否加密并在受保护的位置存储。		✓	✓	2.21
16	忘记的密码和其他恢复路径使用一个TOTP或其他软令牌、移动推送或其他离线恢复机制。在电子邮件或短信中使用随机值通常是最后选择的手段，其存在已知脆弱性。	✓	✓	✓	2.22
17	验证帐号锁定是否分为锁定和锁死状态，它们不是互斥的。如果由于暴力攻击导致帐户暂时被锁定，则不应重置为锁死状态。		✓	✓	2.23
18	验证如需基于问题的共享知识（也称为“秘密问题”），那么这些问题不应违反隐私法律，并且足够强壮以保护帐户免受恶意恢复。	✓	✓	✓	2.24

第 4 章 V2：认证

序号	验证要求描述	1级	2级	3级	原文序号
19	验证系统是否配置密码记忆功能，即不允许重复使用之前的密码。		✓	✓	2.25
20	验证基于风险的双重认证、双因素认证或交易签名应切实地应用到高价值的交易处理中。		✓	✓	2.26
21	验证是否已采取措施来阻止常用的密码和弱密码的使用。	✓	✓	✓	2.27
22	验证所有认证挑战（无论成功还是失败）都应在相同的平均响应时间内进行响应。			✓	2.28
23	验证秘密信息、API密钥和密码没有包含在源代码和在线源代码库中。			✓	2.29
24	验证如果应用程序允许用户进行身份验证，需使用双因素身份验证或其他强身份验证或任何类似的方案来提供保护，以防止用户名和密码的泄露。		✓	✓	2.31
25	验证是否不受信任方无法访问管理员接口。	✓	✓	✓	2.32
26	除非基于风险的策略明确禁止，浏览器自动填充和集成密码管理器是允许的。	✓	✓	✓	2.33

第 5 章 V3：会话管理

– 控制目标

- 控制和维护用户与之交互状态的机制，是所有基于Web应用程序的核心组件之一，被称之为会话管理。其被定义为在用户和基于Web的应用程序之间，治理全状态交互的所有控制的集合。
- 确保经验证的应用程序满足如下会话管理的高级别要求：
- 会话对每一个实体来说是唯一的，不能被猜到或被共享；
- 在非活动周期内，当会话不再被需要或超时时，会话将被无效化。

第 5 章 V3：会话管理

序号	验证要求描述	1级	2级	3级	原文序号
1	验证非自定义会话管理器或自定义会话管理器针对所有常见的会话管理攻击均有抵制。	✓	✓	✓	3.1
2	验证会话在用户注销时失效。	✓	✓	✓	3.2
3	验证会话在指定的不活动时间后超时。	✓	✓	✓	3.3
4	验证在可管理配置的最大时段之后会话超时，不论任何行为（绝对超时）。		✓	✓	3.4
5	验证所有需要认证的页面都具有清晰可见的注销功能。	✓	✓	✓	3.5
6	验证在URL、错误消息或日志中绝不能披露会话ID，其包括验证应用程序不支持会话cookie的URL重写。	✓	✓	✓	3.6

第 5 章 V3：会话管理

序号	验证要求描述	1级	2级	3级	原文序号
7	验证所有认证成功和重新认证后，都将生成新的会话和会话ID。	✓	✓	✓	3.7
8	验证仅由应用程序框架所生成的会话ID是否被应用程序识别为活动状态。		✓	✓	3.10
9	验证在正确的活动会话基础上，会话ID需足够长、随机且唯一。	✓	✓	✓	3.11
10	验证存储在cookie里的会话ID，路径针对应用程序和认证会话令牌设置一个合理的限定值，并追加设置“HttpOnly”和“secure”属性。	✓	✓	✓	3.12
11	验证应用程序所限制的有效并发会话数量。	✓	✓	✓	3.16
12	验证有效的会话列表是否显示在帐户配置文件中以及用户间彼此相同。用户应能够终止任何有效的会话。	✓	✓	✓	3.17
13	在成功的更改密码过程后，验证用户是否被提示“选择终止所有有效的会话”。	✓	✓	✓	3.18

第 6 章 V4：访问控制 21

– 控制目标

- 授权是仅获得许可的实体才被授予资源访问的概念。确保经验证后的应用程序满足如下高级别要求：
- 访问资源者持有有效身份证件；
- 用户与一组明确定义的角色和特权关联；
- 角色和权限元数据免受重播或篡改。

第 6 章 V4：访问控制 21

序号	验证要求描述	1级	2级	3级	原文序号
1	验证最小特权的原则：用户应仅能够访问函数、数据文件、URL、控制器、服务和其他资源，它们处理特定的授权，它们使应用程序免受欺骗和提权。	✓	✓	✓	4.1
2	验证对敏感记录的访问是否实施了保护措施，这样只有授权的对象或数据才允许访问（例如：防止用户篡改参数或更改其他用户帐户）。	✓	✓	✓	4.4
3	验证目录遍历是禁用的，除非故意为之。此外，应用程序不应允许发现或泄露文件或目录元数据，例如Thumbs.db、.DS_Store、.git或.svn。	✓	✓	✓	4.5
4	验证访问控制是否以安全的方式显示失败处理。	✓	✓	✓	4.8
5	验证表示层访问控制规则是否在服务器端强制执行。	✓	✓	✓	4.9
6	验证访问控制使用的所有用户和数据属性、策略信息不能被终端用户操纵，除非特别授权。		✓	✓	4.10

第 6 章 V4：访问控制 21

序号	验证要求描述	1级	2级	3级	原文序号
7	验证是否存在集中化机制（包括调用外部授权服务的库），以保护对每种受保护资源的访问。			✓	4.11
8	验证是否可以记录所有访问控制决定，并记录所有失败的决定。		✓	✓	4.12
9	验证应用程序或框架是否使用强大的随机数（抵御CSRF令牌）或具有其他事务处理保护机制。	✓	✓	✓	4.13
10	验证系统能抵御对安全功能、资源或数据的持续访问。例如，考虑使用资源治理器来限制每小时编辑的数量或阻止整个数据库被单个用户独占。		✓	✓	4.14
11	验证应用程序是否具有针对较低价值系统的额外授权（例如：升级或自适应认证）或高价值应用程序的职责隔离，以根据应用程序和过去欺诈的风险执行反欺诈控制。		✓	✓	4.15
12	验证应用程序是否正确强制执行了上下文相关的授权，以禁止通过参数篡改进行未经授权的操作。	✓	✓	✓	4.16

第 7 章 V5：恶意输入处理

– 控制目标

- 最常见的Web应用程序安全性脆弱性是在使用程序输入内容之前，没有正确合理地验证来自客户端或外部环境的输入。这一脆弱性几乎导致了Web应用程序中的所有关键漏洞，如：跨站脚本攻击、SQL注入、解释器注入、locale/Unicode攻击、文件系统攻击和缓冲区溢出。
- 确保经验证后的应用程序满足如下高级别要求：
- 验证所有输入是正确的，符合预期目的；
- 绝不信任来自外部实体或客户端的数据，应该采取相应地处理措施。

第 7 章 V5：恶意输入处理

序号	验证要求描述	1级	2级	3级	原文序号
1	验证运行时环境不易受到缓冲区溢出的影响，或安全控制可预防缓冲区溢出。	✓	✓	✓	5.1
2	验证服务器端输入验证失败是否导致请求被拒绝且被记录。	✓	✓	✓	5.3
3	验证输入验证规则是否强制在服务器端执行。	✓	✓	✓	5.5
4	验证应用程序为所获得的每一类型的数据使用单个输入验证控件。			✓	5.6
5	验证所有SQL查询、HQL、OSQL、NOSQL和存储过程，调用存储过程是否使用预定义的声明语句或参数化查询，以免受SQL注入的影响。	✓	✓	✓	5.10
6	验证应用程序不受LDAP注入的影响，或该安全控制能预防LDAP注入攻击。	✓	✓	✓	5.11

第 7 章 V5：恶意输入处理

序号	验证要求描述	1级	2级	3级	原文序号
7	验证应用程序不受OS Command注入的影响，或者该安全控制可预防OS Command注入攻击。	✓	✓	✓	5.12
8	当使用文件路径时，验证应用程序不受远程文件包含（RFI）或本地文件包含（LFI）的影响。	✓	✓	✓	5.13
9	验证应用程序不受常见的XML攻击的影响，如：XPath查询篡改，XML外部实体攻击和XML注入攻击。	✓	✓	✓	5.14
10	确保放置在HTML或其他Web客户端代码中的所有字符串变量都可以手动进行上下文编码，也可以使用模板自动编码内容，以确保应用程序不受到反射、存储和DOM跨站脚本（XSS）攻击的影响。	✓	✓	✓	5.15
11	如果应用程序框架允许入站请求对模型的参数进行自动化的批量设置请验证诸如“accountBalance”、“role”、“password”之类的安全敏感字段，以免受到恶意的自动化参数绑定。		✓	✓	5.16
12	验证应用程序具有针对HTTP参数污染攻击的防御能力，特别是在应用程序框架不区分请求参数来源（如：GET、POST、Cookie、标题、环境等）的情况下。		✓	✓	5.17

第 7 章 V5：恶意输入处理

序号	验证要求描述	1级	2级	3级	原文序号
13	除服务器端验证之外，用客户端验证作为第二道防线。		✓	✓	5.18
14	验证是否所有输入数据均被验证，不仅是HTML表单字段，而且包含其他所有输入来源，例如：REST调用、查询参数、HTTP头、Cookie批处理文件、RSS种子等；使用积极的验证策略（白名单），然后辅之以灰名单（消除已知的不正确字符串）或拒绝不正确输入（黑名单）。		✓	✓	5.19
15	验证结构化数据是否根据允许的字符，长度和模式等定义模式强被强类型化且被验证， 例如：信用卡号或电话、验证两个相关字段是否合理（例如：验证区域和邮政编码匹配）。		✓	✓	5.20
16	验证非结构化数据是否强制执行通用安全措施实现数据清洗，例如允许的字符和长度，并在特定条件下可能有害的字符应被转义（例如，使用Unicode或单引号编辑的名称，比如，ねこ或O'Hara）。		✓	✓	5.21
17	确保来自WYSIWYG编辑器或类似文件中的不可信HTML已经通过HTML清洗器进行了正确清洗，并根据输入的验证任务和编码任务进行适当的处理。	✓	✓	✓	5.22
18	对于自动转义模板技术，如果UI转义存有缺陷，请确保启用HTML清洗处理。		✓	✓	5.23

第 7 章 V5：恶意输入处理

序号	验证要求描述	1级	2级	3级	原文序号
19	验证从一个DOM传输到另一个DOM上的数据使用了安全的JavaScript方法，例如：使用.innerText和.val。		✓	✓	5.24
20	验证在浏览器中解析JSON时，验证JSON.parse是否用于解析客户端上的JSON。不要使用eval()来解析客户端上的JSON。		✓	✓	5.25
21	验证在会话终止后，经验证的数据已从客户端存储（例如浏览器DOM）中清除。		✓	✓	5.26

第 8 章 V6：密码学安全

– **控制目标**

- 确保经验证的应用程序满足如下高级要求：
- 所有加密模块均以安全的方式失败，错误被正确处理；
- 当需要随机性时，使用合适的随机数生成器；
- 安全的方式管理密钥的访问。

第 8 章 V6：密码学安全

序号	验证要求描述	1级	2级	3级	原文序号
1	验证所有加密模块均以安全的方式失败，在不使oracle padding的情况下处理错误。	✓	✓	✓	7.2
2	使用加密模块批准的随机数生成器，验证所有随机数、随机文件名、随机GUID和随机字符串是不可能被攻击者猜测的。		✓	✓	7.6
3	验证应用程序使用的加密算法已针对FIPS 140-2或同等标准进行了验证。	✓	✓	✓	7.7
4	验证加密模块是否按照已公布的安全策略在其批准模式下运行。			✓	7.8
5	验证对于加密密钥如何管理是否有明确的政策（例如：生成、分发、撤销和过期）。验证此密钥是否在生命周期内正确执行。		✓	✓	7.9

第 8 章 V6：密码学安全

序号	验证要求描述	1级	2级	3级	原文序号
6	验证加密服务的所有用户都不能直接访问密钥材料。隔离加密过程（包括加密密钥），并考虑使用虚拟或物理硬件密钥库（HSM）。			✓	7.11
7	个人可识别信息应被静态加密存储，并确保在可信信道进行通信。		✓	✓	7.12
8	验证内存中维护的敏感密码或密钥材料在不需要的情况下被0重写，以避免存储转存攻击。		✓	✓	7.13
9	验证所有密钥和密码是可替换的，并在安装时间生成或替换。		✓	✓	7.14
10	验证即使在应用程序处于重负荷状态或者在循环中降级的情形下，仍需使用合适的熵值生成随机数。			✓	7.15

第 9 章 V7：错误处理和日志记录

- **控制目标**

- 错误处理和日志记录的主要目标是为用户、管理员和事件响应小组提供有用的反应 。其目标不是为了制造大量的冗余日志，而是高质量的日志。
- 高质量的日志通常包含敏感数据，且必须依据当地数据隐私法律或指令进行合理的保护。这应该包括：
- 如无特殊需求，不要收集或记录敏感信息；
- 确保所有记录的信息得到安全处理，并依据它的数据分类进行合理保护；
- 确保日志不被永远的保存，而是具有尽可能短暂的完整生命周期。
- 日志中是否包含私有或敏感数据，其界限因国家的不同而不同；日志已成为应用程序所持有的最敏感信息之一，而且它本身对攻击者非常具有吸引力。

第 9 章 V7：错误处理和日志记录

序号	验证要求描述	1级	2级	3级	原文序号
1	验证应用程序没有输出有助于攻击者利用且包含敏感信息的错误消息或堆栈跟踪信息，如：会话ID、软件版本、框架版本和个人信息。	✓	✓	✓	8.1
2	验证安全控制中的错误处理逻辑默认是拒绝访问的。		✓	✓	8.2
3	验证安全日志记录控制能成功记录日志，特别是安全相关的失败事件。		✓	✓	8.3
4	验证每个日志事件是否包括必要的信息，以便在事件发生时依据时间节点进行详细的调查取证。		✓	✓	8.4
5	验证包含不受信任数据源的所有事件不会在日志查看软件中执行代码。		✓	✓	8.5
6	验证安全日志是否受到保护以防止未经授权的访问和修改。		✓	✓	8.6

第 9 章 V7：错误处理和日志记录

序号	验证要求描述	1级	2级	3级	原文序号
7	验证应用程序不应记录如下敏感数据： （1）当地隐私法律或法规定义的敏感数据； （2）风险评估后组织定义的敏感数据； （3）可能有助于攻击者利用的敏感认证数据，包括用户的会话标识符、密码、散列或API令牌。		✓	✓	8.7
8	验证所有不可打印的符号和字段分隔符是否在日志条目中正确编码，以防止日志注入。			✓	8.8
9	验证来自受信源和不受信源的日志字段在日志条目中是否可区分。			✓	8.9
10	验证审计日志或类似条件考虑到关键事务的不可否认性。	✓	✓	✓	8.10

第 9 章 V7：错误处理和日志记录

序号	验证要求描述	1级	2级	3级	原文序号
11	验证安全日志是否具有完整性检查或控制，以防止未经授权的修改。			✓	8.11
12	验证日志是否存储在一个不同的分区上，而不是应用程序所运行的日志循环。			✓	8.12
13	时间源应同步，确保日志具有正确的时间。	✓	✓	✓	8.13

第 10 章 V8：数据保护

– **控制目标**

- 健全的数据保护有三个关键要素：保密性、完整性和可用性（CIA）。本标准假定数据保护在受信的系统上实施（例如服务器），该服务器已被加固并具有充分的保护。
- 应用程序必须假设所有用户设备都以某种方式受到威胁。如果应用程序在诸如共享计算机、电话和平板电脑之类的不安全设备上传输或存储敏感信息，则应用程序负责保证存储在设备上的数据实施了加密，且不能被非法地获取，更改或公开。
- 确保经验证的应用程序满足以下高级数据保护要求：
- 机密性：保护数据，防止数据传输和储存过程中未经授权的查看或披露数据；
- 完整性：保护数据，防止攻击者未经授权的恶意创建，更改或删除数据；
- 可用性：当授权用户需要时，数据是可用的。

第 10 章 V8：数据保护

序号	验证要求描述	1级	2级	3级	原文序号
1	验证所有包含敏感信息的表单需禁用客户端缓存，包括自动完成功能。	✓	✓	✓	9.1
2	验证由应用程序处理的敏感数据列表已被识别，并且有一项明确政策是，如何在相关的数据保护指令下对这些数据进行控制、加密和强制执行。			✓	9.2
3	验证所有敏感数据是在HTTP消息体或头中被发送给服务器（如：从不使用URL参数发送敏感数据）。	✓	✓	✓	9.3

第 10 章 V8：数据保护

序号	验证要求描述	1级	2级	3级	原文序号
4	验证应用程序是否根据应用程序的风险设置合适的反缓存标头，例如： Expires: Tue, 03 Jul 2001 06:00:00 GMT Last-Modified: {now} GMT Cache-Control: no-store, no-cache, must-revalidate, max-age=0 Cache-Control: post-check=0, pre-check=0 Pragma: no-cache	✓	✓	✓	9.4
5	验证在被授权的用户访问敏感数据后，存储的所有敏感信息的缓存或临时副本都不会受到未经授权的访问。清除或失效。		✓	✓	9.5
6	验证在需求的保留策略执行结束时，是否有一种方法能从应用程序中删除每种类型的敏感数据。			✓	9.6

第 10 章 V8：数据保护

序号	验证要求描述	1级	2级	3级	原文序号
7	验证应用程序是否使请求中的参数数量最小化，例如：隐藏字段、Ajax变量、Cookie和标头值。		✓	✓	9.7
8	验证应用程序是否有能力检测和报警异常数量的数据收集请求，例如：屏幕抓取。			✓	9.8
9	验证存储在客户端的数据，不包含敏感数据或个人可识别信息PII（例如：HTML5本地存储 、 会话存储 、 IndexedDB、常规Cookie或Flash Cookie）。	✓	✓	✓	9.9
10	如果数据是根据相关的数据保护指令收集的，或者需要访问记录，那么需验证访问敏感数据是否被准确记录。		✓	✓	9.10
11	验证内存中维护的敏感信息，一旦不再需要，就会被零重写，以减轻内存数据污染攻击。		✓	✓	9.11

第 11 章 V9：通信安全 36

– **控制目标**

- 确保经验证的应用程序满足以下高级别要求：
- 传输敏感数据时，使用TLS；
- 请使用强大的加密算法。

第 11 章 V9：通信安全 36

序号	验证要求描述	1级	2级	3级	原文序号
1	验证一条路径构建可以从一个受信任的CA到每个传输层安全（TLS）服务器证书，并且每个服务器证书都是有效的。	✓	✓	✓	10.1
2	验证TLS用于所有连接（包括外部和后端连接），这些连接都是经过身份验证的，也包括敏感数据或函数；并且这些连接不会回退到不安全或未加密的协议。确保最强的替代方案应用了最合适的算法。	✓	✓	✓	10.3
3	验证是否记录了后台TLS连接失败的信息。			✓	10.4
4	验证已使用设定的信任集合及撤销信息，对所有客户端证书建立并验证证书路径。			✓	10.5
5	验证涉及敏感信息或功能的所有与外部系统的连接是否经过认证。		✓	✓	10.6

第 11 章 V9：通信安全 36

序号	验证要求描述	1级	2级	3级	原文序号
6	验证应用程序使用了标准TLS实现，并在经批准的操作模式下运行应用程序。见本章参考文献（2）			✓	10.8
7	验证TLS证书公钥绑定（HPKP）是否使用生产和备份的公钥实现。有关更多信息，请参阅本章参考文献（3）。		✓	✓	10.10
8	验证HTTP严格传输安全性头文件是否包含在所有请求和所有子域中，如：Strict-Transport-Security: max-age = 15724800; includeSubdomains。	✓	✓	✓	10.11
9	验证生产环境中的网站URL是否已提交给Web浏览器供应商维护的严格传输安全域的预加载列表。			✓	10.12
10	确保使用向前加密密码来降低被动攻击者的流量记录。	✓	✓	✓	10.13
11	验证是否启用和配置了正确的认证撤销处理，如在线证书状态协议（OCSP）Stapling。	✓	✓	✓	10.14
12	验证所有证书层次结构中，均使用强壮的算法，密码和协议，包括所选认证机构的根和中间证书。	✓	✓	✓	10.15
13	确认TLS设置与当前的最新实践是一致的，特别是常见配置密码和算法变得不安全的情况下。	✓	✓	✓	10.16

第 12 章　V10：HTTP安全配置

– **控制目标**

- 确保经验证的应用程序满足以下高级别要求：
- 应用程序服务器应在默认配置下，正确且恰当地加固；
- 在内容类型头，HTTP响应需包含安全的字符集。

第 12 章 V10：HTTP安全配置

序号	验证要求描述	1级	2级	3级	原文序号
1	验证应用程序仅接受已定义的HTTP请求方法，例如GET和POST，且未使用的方法（例如：TRACE、PUT和DELETE）应明确地阻止。	✓	✓	✓	11.1
2	验证每一个HTTP响应是否包含指定安全字符集的内容类型标头（例如：UTF-8、ISO 8859-1）。	✓	✓	✓	11.2
3	验证由可信代理或SSO设备添加的HTTP标头（例如：匿名令牌）是否由应用程序进行认证。		✓	✓	11.3
4	验证合适的X-FRAME-OPTIONS标头被用于站点中，其内容不能在第三方X-Frame中被查看。		✓	✓	11.4

第 12 章 V10：HTTP安全配置

序号	验证要求描述	1级	2级	3级	原文序号
5	验证HTTP标头或HTTP响应的任何部分不会暴露系统组件的详细版本信息。	✓	✓	✓	11.5
6	验证所有API响应是否包含X-Content-Type-Options：nosniff和Content-Disposition：attachment; filename =“api.json”（或用于内容类型的其他适当文件名）。	✓	✓	✓	11.6
7	验证内容安全策略（CSPv2）是否合适，其有助于减轻常见的DOM、XSS、JSON和JavaScript注入漏洞。	✓	✓	✓	11.7
8	验证“X-XSS-Protection: 1; mode =block”用来支持浏览器反射的XSS过滤器。	✓	✓	✓	11.8

第 13 章 V11：恶意控件

– **控制目标**

- 确保经验证的应用程序满足以下高级要求：
- 安全和正确地处理恶意行为，以不影响应用程序的其余部分；
- 不要让时间炸弹或其他基于时间的攻击内置于应用程序之中；
- 不要“回拨”到恶意或未经授权的目的地。
- 应用程序不应有后门、“复活节彩蛋”、Salami攻击或遗留可由攻击者控制的逻辑漏洞。
- 恶意代码极为罕见，且难以检测。人工逐行代码审查可以帮助寻找逻辑炸弹，但即使是最有经验的代码审查者也很难找到恶意代码，即使它切实存在着。如果不访问源代码，这个部分工作是不可能完成的。

第 13 章 V11：恶意控件

序号	验证要求描述	1级	2级	3级	原文序号
1	验证所有恶意活动是否被充分沙盒化、容器化或隔离，以延迟并阻止攻击者攻击其他应用程序。			✓	13.1
2	验证应用程序源代码以及第三方库不包含后门、“复活节彩蛋”，以及在验证、访问控制、输入验证、高价值交易的业务逻辑中的逻辑漏洞。			✓	13.2

第 14 章 V12：业务逻辑

– 控制目标

- 确保经验证的应用程序满足以下高级要求：
- 业务逻辑流是连续且有序的；
- 业务逻辑包括对自动化攻击的检测、限制和防治，例如持续的小额资金转移，或一次性添加一百万个朋友，等等；
- 高价值业务逻辑流已考虑了滥用案例和恶意行为者，并且具有防止欺骗、篡改、抵赖、信息泄露和提权的保护。

第 14 章 V12：业务逻辑

序号	验证要求描述	1级	2级	3级	原文序号
1	验证应用程序在有序地步骤下处理业务逻辑流，所有步骤都按照现实的人力时间进行处理，而不是次序颠倒、跳过步骤、处理对象错误或过快的提交事务。		✓	✓	15.1
2	验证应用程序是否具有业务限制，并基于每一个用户正确实施，可配置的警报和对自动或异常攻击的自动响应。		✓	✓	15.2

第 15 章 V13：文件和资源

– **控制目标**

- 确保经验证的应用程序满足以下高级要求：
- 不可信文件数据应以安全的方式进行处理；
- 从不受信任源获取的内容存储在webroot之外，并且仅具有有限的权限。

第 15 章 V13：文件和资源

序号	验证要求描述	1级	2级	3级	原文序号
1	验证URL重定向和转发只允许被列入白名单的目的地址，或当重定向到潜在的不受信内容时显示警告。	✓	✓	✓	16.1
2	验证不受信文件数据提交到应用程序后，不能直接使用文件I/O命令，特别是要预防路径遍历、本地文件包含、文件MIME类型、操作系统命令注入漏洞。	✓	✓	✓	16.2
3	验证从不受信源获得的文件是否为预期的文件类型，且由防病毒扫描程序实施扫描，以防止已知恶意内容的上传。	✓	✓	✓	16.3
4	验证不受信数据不应在inclusion、类加载器、反射功能中使用，以防止远程或本地文件包含脆弱点。	✓	✓	✓	16.4
5	验证不受信数据不在跨域资源共享（CORS）中使用，以防止远程内容被注入任意内容。	✓	✓	✓	16.5

第 15 章 V13：文件和资源

序号	验证要求描述	1级	2级	3级	原文序号
6	验证从不受信源获得的文件是否存储在webroot的外部，且仅具有有限的权限，最好已经过健全的认证。		✓	✓	16.6
7	验证Web或应用程序服务器默认配置为拒绝访问远程资源或在Web和应用程序服务器之外的系统。		✓	✓	16.7
8	验证应用程序不执行来自不可信源的上传数据。	✓	✓	✓	16.8
9	不要使用Flash、Active-x、Silverlight、NACL、客户端Java或其他客户端技术，这些技术与生俱来地不支持W3C浏览器标准。	✓	✓	✓	16.9

第 16 章 V14：移动应用程序

– **控制目标**

- 本节主要针对移动应用程序控件。
- 移动应用应软件：
- 在可信环境中执行安全控制，移动客户端与服务器端应具有相同级别的安全控制；
- 设备上的敏感信息应安全地存储；
- 设备中传输的敏感信息应在传输层以安全的方式进行传输。

第 16 章 V14：移动应用程序

序号	验证要求描述	1级	2级	3级	原文序号
1	验证存储在设备上并可由其他应用程序检索的ID值（例如：UDID、IMEI号码），不用作认证令牌。	✓	✓	✓	17.1
2	验证移动应用不应将敏感数据存储在设备未加密的共享资源上（例如：SD卡、共享文件夹）。	✓	✓	✓	17.2
3	验证敏感数据不应存储在未受保护的设备上，即使在诸如密钥链之类的系统保护区域也是如此。	✓	✓	✓	17.3
4	验证密钥、API令牌、密码应在移动应用程序中动态生成。	✓	✓	✓	17.4
5	验证移动应用程序是否防止敏感信息的泄露（例如：当应用程序在后台或在控制台编写敏感信息时，屏幕截图被保存了下来）。		✓	✓	17.5
6	验证应用程序是否要求所需功能和资源的权限最小化。		✓	✓	17.6

第 16 章 V14：移动应用程序

序号	验证要求描述	1级	2级	3级	原文序号
7	验证应用程序敏感代码在内存中不可预测地布局（例如ASLR）。	✓	✓	✓	17.7
8	验证是否存在反调试技术足以阻止或延迟可能的攻击者将调试器注入到移动应用程序中。			✓	17.8
9	验证该应用程序不会对同一设备上的其他移动应用程序导出敏感活动、内容或内容提供商。	✓	✓	✓	17.9
10	验证内存中维护的敏感信息，一旦不再需要，是否会用零重写，以减轻内存转储攻击。		✓	✓	17.10
11	验证该应用程序是否对输入进行验证，确认活动的导出、内容或内容提供者属性。	✓	✓	✓	17.11

第 17 章　V15：WEB服务50

– 控制目标

- 基于Web服务，使用RESTful或SOAP的应用程序，经验证后需保证如下要求：
- 针对所有Web服务，进行充分的认证，会话管理和授权；
- 从较低信任级向高信任级别的转换时，需针对所有参数进行输入验证；
- SOAP Web服务层应具备互操作性，以促进API的使用。

第 17 章 V15：WEB服务50

序号	验证要求描述	1级	2级	3级	原文序号
1	验证在客户端和服务器之间使用相同的输出编码风格（encoding style）。	✓	✓	✓	18.1
2	验证Web服务应用程序中，对管理员和管理功能的访问仅限于Web服务管理员。	✓	✓	✓	18.2
3	验证XML或JSON模式是否恰当并在接受输入之前进行验证。	✓	✓	✓	18.3
4	验证所有输入是否限制在合适的长度。	✓	✓	✓	18.4
5	验证基于SOAP的Web服务至少要符合Web服务-互操作性（WS-I）基本配置文件，即TLS加密的实施。	✓	✓	✓	18.5

第 17 章 V15：WEB服务50

序号	验证要求描述	1级	2级	3级	原文序号
6	验证基于会话的认证和授权的使用。请参阅第2节、第3节和第4节 ，以获得进一步的指导。避免使用静态“API键”等。	✓	✓	✓	18.6
7	验证REST服务是否受到跨站点请求伪造的保护，通过至少一个或多个以下内容：ORIGIN checks、double submit cookie pattern、CSRF nonces和referrer checks.	✓	✓	✓	18.7
8	验证REST服务是否明确检查传入的Content-Type为预期的内容，例如application / xml或application / json。		✓	✓	18.8
9	验证消息有效负载是否被签名以确保客户端和服务之间的可靠传输，使用JSON Web Signing或WS-Security进行SOAP请求。		✓	✓	18.9
10	验证可替代和不太安全的访问路径不存在。		✓	✓	18.10

第 18 章 V16：安全配置

– **控制目标**

- 确保经验证的应用，满足如下要求：
- 最新的类库和平台；
- 默认安全配置；
- 有效地控制和防护用户对默认配置的更改，避免不必要的披露或给底层系统造成安全漏洞或缺陷。

第 18 章 V16：安全配置

序号	验证要求描述	1级	2级	3级	原文序号
1	所有组件都应为最新的，并具有适当的安全配置和版本。这应包括删除不需要的配置和文件夹，如：示例应用程序、平台文档、默认或示例用户。	✓	✓	✓	19.1
2	组件之间的通信，例如：应用程序服务器和数据库服务器之间的通信应该被加密，特别是当组件在不同的容器中或在不同的系统上时。		✓	✓	19.2
3	组件之间的通信，例如：应用程序服务器和数据库服务器之间的通信应使用最小权限帐户进行认证。		✓	✓	19.3
4	验证应用程序部署是否充分地沙盒化、容器化和隔离化，以延迟并阻止攻击者攻击其他应用程序。		✓	✓	19.4

第 18 章 V16：安全配置

序号	验证要求描述	1级	2级	3级	原文序号
5	验证应用程序构建和部署过程以安全的方式执行。		✓	✓	19.5
6	验证授权管理员是否有能力核实所有安全相关配置的完整性，以确保它们未被篡改。			✓	19.6
7	验证所有应用程序组件已签名。			✓	19.7
8	验证第三方组件是否来自受信的存储库。			✓	19.8
9	验证系统级语言的构建过程是否启用了所有安全标签，例如：ASLR、DEP、安全检查。			✓	19.9
10	验证应用程序资源是否被托管，例如：JavaScript库、CSS样式表、Web字体由应用程序托管，而不是依赖于CDN或外部提供者。			✓	19.10

第 19 章　ASVS的实践案例

- 19.1　案例1：作为安全测试指南使用

　　美国犹他州私立大学校园RedTeam对校园各部门网络和应用程序进行渗透测试。

- 19.2　案例2：作为SDLC的实施指导

　　为金融机构大数据建设提供基础性安全支持。

Thanks !